ICT-risicobeheer met DORA

mr. T.W.G. de Wit en Mr. G. Verschuuren EMoC RMFI[1]

Op 17 januari 2025 treedt de Digital Operational Resilience[2] Act ("DORA" of "Verordening")[3] voor de financiële sector in werking. DORA is een Europese Verordening en gaat kort gezegd over informatiebeveiliging. DORA vereist van financiële entiteiten dat zij bestand zijn tegen en reageren op ICT-gerelateerde verstoringen en bedreigingen en deze spoedig kunnen herstellen.

DORA is een gedetailleerd en omvangrijk wetgevingspakket en financiële entiteiten dienen tijdig te starten met de voorbereiding op de inwerkingtreding van DORA. In dit artikel bespreken we de achtergrond, doelstelling en inhoud van DORA. Hierbij hebben wij met name aandacht voor het ICT-risicobeheer. Dit is de belangrijkste pijler binnen DORA en wat ons betreft begint de voorbereiding op DORA met het vaststellen en implementeren van een solide ICT risicobeheerraamwerk. Ook bekijken we kort hoe DORA zich verhoudt tot reeds eerder door DNB en AFM gepubliceerde guidance op dit gebied. Tot slot staan we kort stil bij relevante ontwikkelingen in de Verenigde Staten. We ronden af met enkele slotbeschouwingen.

1. Introductie DORA

1.1. Digital Finance Package

DORA maakt deel uit van het Digital Finance Package ("DFP") van de Europese Commissie.[4] Het DFP beoogt een competitieve Europese financiële sector te bevorderen die consumenten toegang biedt tot innovatieve financiële producten, waarbij consumentenbescherming en financiële stabiliteit geborgd zijn. Het DFP is onderdeel van de ambitie van de Europese Unie om de digitale transitie te omarmen, en zo Europa tot een digitale wereldspeler te maken. Het DFP bevat hiertoe een digitale financiële strategie, wetsvoorstellen met betrekking tot crypto-assets, een strategie voor retail betalingsverkeer en een wetsvoorstel voor een EU toezichtraamwerk ten aanzien van digitale operationele veerkracht (DORA dus).

Digitalisering en operationele veerkracht in de financiële sector zijn twee kanten van dezelfde medaille. Digitale technologieën of informatie- en communicatietechnologieën (ICT) worden inmiddels over de hele breedte van de financiële sector ingezet en brengen zowel kansen als risico's mee. Die risico's houden zich niet aan landsgrenzen; een systeemkwetsbaarheid kan zich snel door de hele Unie verspreiden. DORA moet zorgen voor een gedetailleerd en alomvattend kader voor digitale operationele veerkracht van financiële entiteiten in de EU.[5]

1.2. Opzet DORA

DORA is geen toegankelijke verordening, nu zij bol staat van complexe terminologie en abstracte definities. DORA valt in de volgende hoofdstukken uiteen:

I. Algemene bepalingen
II. ICT risicobeheer
III. ICT-gerelateerde incidenten, Beheer, Classificatie en Rapportage
IV. Testen van digitale operationele veerkracht
V. Beheer van ICT risico van derde aanbieder
VI. Regelingen voor informatie-uitwisseling
VII. Bevoegde autoriteiten
VIII. Gedelegeerde handelingen
IX. Overgangs- en slotbepalingen

Met name de hoofdstukken II, III, IV en V voorzien in de materiële regels. In dit artikel richten wij ons zoals gezegd op ICT-risicobeheer, hoofdstuk II van DORA. Dat wil overigens niet zeggen dat de andere hoofdstukken helemaal geen betrekking hebben op ICT-risicobeheer. Incidentenbeheer, testen van digitale operationele veerkracht en het beheer van ICT-risico's van derde aanbieders, gaan in feite net zo goed over ICT risicobeheer. Het betreft dan concrete

1. Gijs Verschuuren is Chief Risk Officer van IBS Capital Allies, Tim de Wit is advocaat bij Finnius. De auteurs danken Ralf Siebelt CISSP voor zijn suggesties. Dit artikel is afgerond op 23 april 2023.
2. Onder 'operationele digitale weerbaarheid' wordt op grond van artikel 3 sub (1) Verordening verstaan het vermogen van een financiële entiteit om haar operationele integriteit uit technologisch oogpunt op te bouwen, te waarborgen en te evalueren, door direct of indirect via gebruik van diensten van derde ICT-aanbieders te voorzien in het volledige scala van ICT-gerelateerde capaciteiten die nodig zijn voor de beveiliging van de netwerk- en informatiesystemen waarvan een financiële entiteit gebruikmaakt, en die de permanente verlening van financiële diensten en de kwaliteit ervan ondersteunen.
3. Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 (*PbEU* 2022, L 333/1).
4. Zie de overzichtspagina van de Europese Commissie; raadpleegbaar via: https://finance.ec.europa.eu/publications/digital-finance-package_en.
5. Zie onder meer overweging (1), (2) en (3) Verordening.

invulling van het ICT-risicobeheerraamwerk op specifieke deelonderwerpen.

Veel van de bepalingen in DORA worden overigens nog verder uitgewerkt in lagere regelgeving, zoals gedelegeerde verordeningen. Daar zullen we de komende tijd voorstellen voor gaan zien vanuit de Europese toezichthouders. Opvallend genoeg is de uiterlijke termijn voor concept voorstellen ter indiening bij de Europese Commissie pas 17 januari 2024.[6] Die moeten daarna nog definitief worden aangenomen. In potentie moeten marktpartijen dus lang wachten op de definitieve lagere regelgeving. De Europese toezichthouders hebben wel al aangegeven in de loop van dit jaar met een consultatie te komen[7], op basis waarvan hopelijk al kan worden opgemaakt welke richting de Europese toezichthouders op willen met de lagere regelgeving. Gezien de vereiste voorbereiding op DORA raden we marktpartijen niet aan te wachten op de definitieve lagere regelgeving, maar alvast te beginnen met voorbereiding en daarbij te putten uit de eerste voorstellen vanuit de Europese toezichthouders.

1.3. Reikwijdte

DORA is cross-sectorale regelgeving en raakt zodoende veel verschillende type instellingen. DORA is van toepassing op een breed scala aan financiële entiteiten, waaronder kredietinstellingen, beleggingsondernemingen, fondsbeheerders, aanbieders en emittenten van cryptovaluta, (her)verzekeringsondernemingen, ratingbureaus en aanbieders van crowdfundingsdiensten.[8]

Daarnaast bevat DORA regels voor zogenoemde 'derde aanbieders van ICT-diensten'. Dat zijn ondernemingen die digitale en datadiensten aanbieden, met inbegrip van aanbieders van cloudcomputingdiensten, software, gegevensanalysediensten en datacentra. Denk bijvoorbeeld aan big tech ondernemingen zoals Google, Amazon en Microsoft. Deze laten we verder buiten beschouwing.

1.4. Proportionaliteit

DORA is een *one-size-fits-all* raamwerk en in principe op iedere entiteit gelijkelijk van toepassing ongeacht of, bijvoorbeeld, een entiteit nu een kredietinstelling of fondsbeheerder is. DORA voorziet echter wel in de mogelijkheid van een zekere proportionele toepassing. Artikel 4 lid 1 Verordening bepaalt dat financiële entiteiten de verplichtingen uit hoofdstuk II inzake ICT-risicobeheer moeten toepassen rekening houdend met hun omvang, algehele risicoprofiel en de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen.

Het is op grond van DORA niet duidelijk wat dit precies betekent voor naleving van de eisen. Het is daarbij de vraag of DNB en AFM gegeven de aard van de risico's die DORA tracht te beheersen veel zullen voelen voor een proportionele toepassing.[9] Een proportionele toepassing zou zeker voor de wat kleinere financiële instellingen wat lucht bieden. Dat eventueel beroep op proportionaliteit zou dan naar onze mening met name moeten worden gegrondvest op de specifieke, beperkte, ICT-risico's die relevant zijn voor de betreffende financiële entiteit en niet enkel op de omvang van die onderneming. Dit zou op kunnen gaan voor entiteiten die beperkt gebruik maken van digitale en ICT-technologieën of uitsluitend hiervan gebruikmaken voor niet-materiële bedrijfsprocessen. Gezien de brede digitalisering binnen de financiële sector is de vraag hoe houdbaar zo'n beroep is en blijft. Het zou voor de markt wenselijk zijn als DNB en de AFM handvatten zouden aanreiken hoe marktpartijen een beroep op proportionaliteit kunnen inkleden.

Daarnaast zijn zogenoemde "micro-ondernemingen" uitgezonderd van bepaalde eisen van DORA. Een micro-onderneming is een onderneming waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal EUR 2 miljoen niet overschrijdt.[10] De vraag is dus sterk wat het belang van deze uitzondering is voor de praktijk. Tot slot zijn er voor bepaalde specifieke financiële entiteiten uitzonderingen beschikbaar[11], waar we nu verder niet op ingaan.[12]

6. Artikel 15 Verordening.
7. Zie de door de Europese toezichthouders gegeven presentatie tijdens een *public hearing* op 6 februari 2023, raadpleegbaar via: https://www.eba.europa.eu/calendar/joint-esas-public-event-dora-%e2%80%93-technical-discussion.
8. Artikel 2 lid 1 Verordening.
9. Zie bijvoorbeeld ook DNB studie proportioneel en effectief toezicht, pagina 7: "Omvang zou dus nooit het enige criterium mogen zijn waarmee wordt bepaald of instellingen voor vereenvoudigde of lagere eisen in aanmerking komen. Het bedrijfsmodel van kleine instellingen gaat niet automatisch met lage risico's gepaard en kan derhalve wel degelijk veel prudentiële aandacht vereisen.", https://www.dnb.nl/media/yojpc5a5/dnb-studie-proportioneel-en-effectief-toezicht.pdf
10. Artikel 3 onder 60) Verordening.
11. Artikel 16 Verordening. Het gaat om kleine en niet-verweven beleggingsondernemingen en bepaalde vrijgestelde betaaldienstverleners, elektronischgeldinstellingen en kleine instellingen voor bedrijfspensioenvoorziening.
12. De vraag kan daarmee rijzen, of er een risico op ongelijke toezichtsrechtelijke behandeling bestaat voor dergelijke deels uitgezonderde ondernemingen. Dat risico lijkt ons beperkt, gegeven de hoge mate van ICT gebruik binnen de financiële sector als ook de concentratietendens bij kritische uitbestedingen (zie ook Terugkoppeling onderzoek Uitbestedingsrapportage Beleggingsondernemingen en Beheerders, brief van de AFM d.d. 21 juli 2021). We vragen ons met andere woorden a priori af, of de verschillen in relevant ICT risico voor deze partijen onderling nu zo verschillen.

2. ICT-risicobeheer

Hoofdstuk II (artikel 4 tot en met 14) van DORA heeft betrekking op ICT-risicobeheer. Een ICT-risico is in DORA gedefinieerd als '*elke redelijkerwijs aan te wijzen omstandigheid met betrekking tot het gebruik van netwerk- en informatiesystemen die, indien zij zich voordoet, de beveiliging van het netwerk- en informatiesysteem, van technologieafhankelijke instrumenten of processen, van verrichtingen en processen, of van de levering van de diensten in gevaar kan brengen, door schadelijke effecten met zich mee te brengen in de digitale of fysieke omgeving*'.[13] Het gaat hier dus om een breed spectrum van ICT risico's: zowel hardware als software, zowel systemen als apparatuur, netwerkverbindingen en interfaces, uitval, verstoringen, verkeerd gebruik, data en cybersecurity (etc.).

2.1. Governance en organisatie

Artikel 4 Verordening verplicht financiële entiteiten te beschikken over interne governance- en controlekaders die een doeltreffend en prudent beheer van alle ICT-risico's waarborgen.[14] In dit kader legt DORA het leidinggevend orgaan van een instelling negen verplichtingen op. De definitie van leidinggevend orgaan als gebezigd in DORA omvat in een Nederlandse context in beginsel zowel het bestuur als de raad van commissarissen. Onder de genoemde negen verplichtingen[15] worden geschaard de eindverantwoordelijkheid voor het beheer van de ICT-risico's, de vaststelling van duidelijke taken en verantwoordelijkheden voor alle ICT-gerelateerde functies en het bepalen van het passende risicotolerantieniveau voor het ICT-risico (de zogenaamde *risk appetite*[16]).[17] Het ligt daarmee naar ons oordeel in de rede dat het bestuur primair verantwoordelijk is voor naleving van deze verplichtingen en dat de raad van commissarissen daar toezicht op houdt.

Een andere verplichting in dit kader betreft de toewijzing en de periodieke evaluatie van het passende budget. Hieronder worden ook opleidingskosten begrepen.[18] Dit is een op zichzelf logische verplichting, zonder toereikend budget bereik je niet veel. In de praktijk kan deze verplichting nog wel tot hoofdbrekens leiden. Naast de gebruikelijke budgetallocatie die voor alle activiteiten heeft te gelden, zijn niet alle ICT-risico's (met name cybersecurity) even makkelijk budgettair te vertalen.[19] Daarnaast geldt – net als voor veel andere risico's – ook voor ICT-risico's, dat de (potentiële) opbrengsten van het nemen van maatregelen moeilijk te kwantificeren zijn.[20]

Het is de vraag, of het bestuur van een financiële entiteit, met op sommige plekken mogelijk nog latente affiniteit met ganzenveer en trekschuit in plaats van met de laatste technologische ontwikkelingen, in alle gevallen op deze taak berekend is. Kennelijk ziet de wetgever die bui ook al hangen, aangezien artikel 5 lid 4 DORA bepaalt dat leden van het bestuur regelmatig specifieke opleidingen moeten volgen teneinde voldoende kennis en vaardigheden te verwerven en te onderhouden om ICT-risico's en de gevolgen daarvan voor de activiteiten van de financiële entiteit te begrijpen en te beoordelen.[21] Het is sterk aan te raden dat het bestuur die opleiding al *voorafgaand* aan inwerkingtreding van DORA afneemt, aangezien zij dan ook in staat is om de implementa-

13. Artikel 3 onder 4 Verordening.
14. Artikel 3:17 Wet op het financieel toezicht (Wft) verplicht hier feitelijk ook al toe.
15. Artikel 5 lid 2 Verordening.
16. Risk Appetite is de mate van risico die een onderneming bereid is te lopen om haar doelstellingen te verwezenlijken. Risk Appetite is daarmee sterk gekoppeld aan de strategie van een onderneming. Risk Appetite valt op meerdere risiconiveaus te bepalen: zowel ten aanzien van de onderneming als geheel, als op hoofdrisicocategorieën (strategisch risico, financieel risico en niet-financieel (operationeel) risico), als op subrisicogebied (renterisico, fraude, etc.). Risk Appetite hoeft niet altijd heel precies met metrics of Key Risk Indicators omschreven te worden. Vergelijk de twee volgende Risk Appetite Statements, de eerste wat algemener en de tweede preciezer omschreven (beide voorbeelden ontleend aan COSO Guidance Risk Appetite, p.25, https://www.coso.org/Shared%20Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf). Risk Appetite Statement 1: *Echo Relief, a service organization to help people through disasters, will pursue new programs that enhance the delivery of services to those in need within our financial ability. We will accept moderate risk to the safety of staff and volunteers as we respond to disasters. In order to maintain good stewardship of donor funds, we have a low appetite for risks related to misuse of funds.* Risk Appetite Statement 2: *We are not comfortable accepting more than a 10% probability that we will incur losses of more than $1 million in pursuit of a specific objective.*
17. De herziene EBA Richtsnoeren inzake uitbesteding van 25 februari 2019 (EBA/GL/2019/02) kennen vergelijkbare verplichtingen ten aanzien van risicobeheer en de rol die het leidinggevend orgaan van de betreffende instelling. Zie de artikelen 32-38.
18. Artikel 5 lid 2 sub g Verordening.
19. Ter illustratie: het wordt steeds lastiger en duurder om een cybersecurity verzekering af te sluiten, omdat veel van de te verzekeren risico's erg lastig te beprijzen zijn. Zie https://www.verzekeraars.nl/verzekeringsthemas/schade/cyber en https://www.consultancy.nl/nieuws/40726/kosten-van-een-cyberverzekeringen-worden-fors-hoger.
20. Daar bestaan wel enkele, niet eenvoudige, technieken voor zoals ROM (return on mitigation). Hierbij worden de kosten van een maatregel vergeleken met de financiële impact als een asset (zoals een netwerk) wordt gecompromitteerd. Zie voor enkele andere technieken: https://www.csoonline.com/article/3229887/how-to-calculate-your-return-on-security-investments.html.
21. Zie ook de Handreiking Digitale continuïteit en weerbaarheid op de bestuurstafel, met tips voor CISO's en IT lijnmanagers om informatiebeveiliging op de bestuursagenda te krijgen: https://www.digitaltrustcenter.nl/sites/default/files/2022-11/Agentschap%20Telecom%20-%20Handreiking_TG_.pdf.

tie van DORA goed te overzien.[22] Ook leden van de raad van commissarissen zullen zich bekend moeten maken met de verplichtingen uit hoofde van DORA en impact voor de financiële entiteit ten einde te kunnen voldoen aan hun toezichthoudende taken.

2.2. Kader voor ICT-risicobeheer

Financiële entiteiten moeten beschikken over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer[23], dat hen in staat stelt ICT-risico's snel, efficiënt en zo volledig mogelijk aan te pakken en een hoog niveau van digitale operationele veerkracht te waarborgen dat overeenstemt met hun zakelijke behoeften, omvang en complexiteit.[24] Dit kader heeft ook betrekking op de bescherming van gebouwen en hardware.[25] Dat kan zich vertalen in maatregelen op het gebied van fysieke toegangsbeveiliging (niet iedereen heeft toegang tot alle ruimten), ongeoorloofd gebruik van assets[26], en ook op brandbeveiliging en fysiek afgescheiden servers.
Financiële entiteiten moeten de ICT-risico's tot een minimum beperken door passende strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten in te zetten.[27] Het is lastig een dergelijke abstracte verplichting concreet te maken. Per ICT-risico zal bekeken moeten worden wat een passende maatregel is om het risico te mitigeren. Ten aanzien van de ICT-beveiliging van de organisatie als geheel, kunnen financiële entiteiten kijken naar de ISO 27001 norm op het gebied van *Information security, cybersecurity and privacy protection*[28].
Entiteiten dienen een passende scheiding van ICT-beheerfuncties, controlefuncties en interne auditfuncties te garanderen, overeenkomstig het model van de drie verdedigingslijnen (*Three Lines of Defense*-model)[29] of een model voor intern risicobeheer en -controle.[30] Het Three Lines of Defense-model wordt voor zover wij weten door vrijwel alle Nederlandse financiële instellingen gebruikt, en is aldus ook bij toezichthouders AFM en DNB een bekend en geaccepteerd model.[31] DORA laat echter ook ruimte deze scheiding op een andere wijze te bewerkstelligen.[32] Het kader moet periodiek worden beoordeeld door auditors, die over voldoende kennis en ervaring moeten beschikken op het gebied van ICT-risico's.[33] Daarbij dient een formeel follow-upproces te worden gevolgd met regels voor de tijdige verificatie en remediëring van kritieke ICT-auditbevindingen.[34] Daarmee dwingt DORA in feite tot instelling van een interne auditfunctie, terwijl die voor bepaalde onder toezicht staande instellingen op basis van het beginsel van proportionaliteit niet altijd verplicht hoeft te zijn.[35] Wij menen dat het beginsel van proportionaliteit zoals hiervoor besproken hier soelaas zou kunnen bieden, terwijl ook gedacht kan worden aan een "externe" internal audi-

22. Het is bij de vereiste deskundigheid van het bestuur de vraag, of deze verplichting rust op het bestuur als geheel of op iedere individuele bestuurder. De AFM lijkt zich in ieder geval op het standpunt te stellen, dat iedere bestuurder ten minste enige kennis van DORA zou moeten hebben (zie het artikel van AFM voorzitter Laura van Geest in het FD d.d. 16 april 2023: "Bestuurders kunnen het niet langer van zich afschuiven en overlaten aan de cyberexperts"). Wij denken dat het te ver voert van iedere bestuurder te verlangen diepgaande kennis van DORA en cybersecurity te hebben. In die zin kan er best één expert in het bestuur zitten. Maar de overige bestuurders moeten wel een basiskennis hebben en de risico's kunnen beoordelen en een gevoel van *urgency* te waarborgen. De verplichting om passend budget te alloceren aan digitale operationele weerbaarheid ingevolge artikel 5 lid 2 sub g DORA zorgt in ieder geval voor periodieke aandacht voor het onderwerp.
23. Nadere uitwerking vindt plaats in artikel 6 lid 8 DORA.
24. Artikel 6 lid 1 Verordening.
25. Artikel 6 lid 2 Verordening.
26. Dit kan enerzijds worden geregeld door fysieke toegangsbeveiliging, zodat slechts een beperkte groep toegang heeft tot een specifieke asset of ruimte, anderzijds vaak ook door autorisatiematrices. Hierin wordt bepaald tot welke systemen en applicaties iemand toegang krijgt, vaak gebaseerd op de rol / functieprofiel in de betreffende organisatie.
27. Artikel 6 lid 3 Verordening.
28. Zie in dit verband: https://www.iso.org/obp/ui#iso.
29. Zie ook https://www.bis.org/bcbs/publ/d328.htm. Wij lezen deze DORA verplichting aldus, dat er sprake moet zijn van functiescheiding tussen ICT beheer (eerste lijn), de controlefuncties (tweede lijn) en audit functie (derde lijn). Dat zou ook het geval (moeten) zijn als niet van het Three Lines of Defense model gebruik gemaakt wordt. In die zin voegt deze bepaling niet zoveel toe. Wij lezen deze verplichting niet, dat er een separate functionaris voor ICT-beheer zou moeten worden benoemd.
30. Artikel 6 lid 4 Verordening.
31. Dit betekent trouwens niet, dat de invulling van dat model bij alle instellingen volledig inwisselbaar is. Met name de rolverdeling tussen eerste en tweede lijn kan variëren afhankelijk van hoe de organisatie intern is ingericht qua (omvang van) activiteiten en personeel. Ook hangt dit af van de volwassenheid van de organisatie, en de wijze waarop de Risk Management en Compliance functies hun taken en verantwoordelijkheden invullen. Het is goed hierbij voor ogen te houden, dat risicomanagement zowel in de eerste als in de tweede lijn wordt uitgevoerd. In de klassieke invulling van het Three Lines of Defense model wordt kort gezegd het dagelijkse risicomanagement door de eerste lijn uitgevoerd, en gecontroleerd door de tweede lijn. Dat is direct een bezwaar tegen het model, omdat het voor de tweede lijn (zonder aanpassingen op het model) erg lastig is proactief en preventief te acteren.
32. Het Three Lines of Defense model kent zijn beperkingen en kan een voedingsbodem vormen voor veel bureaucratie: zie E.E.O. Roos Lindgreen en D. Daams, 'Internal audit: waker, slaper of dromer?', Maandblad Voor Accountancy en Bedrijfseconomie 2020, 94(3/4): 81-82, raadpleegbaar via: mab-online.nl/article/49595/.
33. Artikel 6 lid 6 Verordening. Zie ten aanzien van invulling van de auditwerkzaamheden de Handreikingen van NOREA (de Nederlandse beroepsorganisatie van IT-auditors): https://www.norea.nl/handreikingen.
34. Artikel 6 lid 7 Verordening.
35. Wij denken bijvoorbeeld aan beheerders met vergunning op grond van de *Alternative Investment Fund Managers Directive*.

tor (sommige accountants bieden deze dienstverlening aan).[36]

2.3. ICT-systemen, -protocollen en -instrumenten

Op grond van artikel 7 Verordening dienen financiële entiteiten geactualiseerde ICT-systemen, -protocollen en -instrumenten te gebruiken en onderhouden.[37] Deze moeten zijn afgestemd op de activiteiten van de entiteit, moeten betrouwbaar zijn en moeten ook in staat zijn piekbelastingen op te vangen dan wel als back-up kunnen fungeren bij de implementatie van nieuwe technologie.

2.4. Identificatie

In het kader van het ICT-risicobeheer identificeren, classificeren en documenteren financiële entiteiten ten minste jaarlijks alle door ICT ondersteunde bedrijfsfuncties, taken en verantwoordelijkheden, de informatie[38]- en ICT-activa[39] die deze functies ondersteunen, en hun taken en afhankelijkheden met betrekking tot ICT-risico's.[40]
Dit artikel onderscheidt aldus identificatie, classificatie en documentatie. Met identificatie wordt gedoeld op het in beeld hebben van alle bedrijfsfuncties door ICT ondersteund worden. Denk bijvoorbeeld aan medewerkers van de trading desk van een bank die van software gebruik maken voor het uitvoeren van transacties. De entiteit moet aldus ook alle binnen de entiteit aanwezige hardware en software die ondersteunend zijn aan die bedrijfsfuncties identificeren. Dat klinkt als een open deur, maar kan in de praktijk nogal tegenvallen.[41] Grotere financiële entiteiten hebben honderden systemen en applicaties lopen, om nog maar te zwijgen van tienduizenden apparaten die in gebruik zijn (servers, netwerkapparatuur, computers en telefoons bijvoorbeeld). Zonder een goede identificatie kunnen kwetsbaarheden onopgemerkt blijven, bijvoorbeeld applicaties die draaien op verouderde software of laptops die door voormalige medewerkers mee naar huis zijn genomen. Die vormen dan een beveiligingsrisico, en dat is precies wat DORA beoogt te voorkomen. Hierbij moet bedacht worden, dat ook informatie activa die niet bij de primaire processen behoren een beveiligingsrisico kunnen vormen: zo is in de Verenigde Staten in 2018 een casino gehackt via de met het internet verbonden thermometer van het aquarium.[42]
Niet het eerste waar je aan denkt bij een activa identificatie. Een dergelijke identificatie leidt in de regel tot een IT-inventaris, waarmee direct ook het punt "documentatie" (voor een deel) geraakt wordt.
Met classificatie wordt bedoeld, dat informatie een bepaald risico- of beschermingsniveau krijgt. Dit beschermingsniveau is afhankelijk van het belang van die informatie voor de (kritische) bedrijfsprocessen. Het is gebruikelijk een classificatie uit te voeren op basis van de factoren beschikbaarheid (continuïteit), integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit).[43] Deze classificatiemethodiek wordt ook wel BIV[44] genoemd.[45,46]
De factor Beschikbaarheid komt neer op continuïteit (is de informatie beschikbaar als het nodig is, ook tijdens storingen en piekbelastingen). De factor Integriteit komt erop neer, dat informatie tijdig beschikbaar is, juist en volledig is, en niet ongeautoriseerd of onopgemerkt kan worden aangepast, achtergehouden of verwijderd. Vertrouwelijkheid heeft vooral betrekking op de kring van personen die toegang tot bepaalde data hebben en hoe er met die data moet worden omgegaan. Alle relevante informatie en systemen dienen dan een dergelijke BIV classificatie te krijgen.[47]
Verder vereist artikel 8 lid 2 Verordening dat financiële entiteiten permanent alle bronnen van ICT-risico identificeren, met name de wederzijdse risicoblootstelling ten aanzien van andere financiële

36. Dit leidt in onze optiek niet tot tweede orde effecten in de zin van dat de externe internal auditor als derde aanbieder van ICT-diensten kan worden gezien. De controleactiviteiten zijn niet als ICT-diensten als bedoeld in artikel 3 sub 21 DORA te beschouwen. Bovendien betreft het veelal een detachering van één of meerdere specifieke personen die onder verantwoordelijkheid van de financiële entiteit werken, in plaats van een uitbesteding aan een externe dienstverlener.
37. Een voorbeeld hiervan is een Security Information and Event Management (SIEM) technologie. SIEM-technologie verzamelt gebeurtenislogboekgegevens uit een reeks bronnen, identificeert afwijkende activiteiten en kan eventueel (semi)autonoom ingrijpen.
38. Artikel 3 onder 4) Verordening definieert een 'informatieactief' als: een reeks, al dan niet tastbare, gegevens die beschermenswaardig zijn.
39. Artikel 3 onder 5) Verordening definieert een 'ICT-actief' als: een software- of hardwareactief in de netwerk- en informatiesystemen die door de financiële entiteit worden gebruikt.
40. Artikel 8 lid 1 Verordening.
41. Dat geldt zeker bij uitbestede dienstverlening. Met name het actueel houden van het activa-overzicht is dan een hele toer, nog afgezien van het feit dat lang niet alle derde dienstverleners altijd kunnen of willen meewerken.
42. Zie voor een verdere toelichting: https://thehackernews.com/2018/04/iot-hacking-thermometer.html.
43. Zie ook: https://www.nationaleombudsman.nl/system/files/bijlage/BIR_TNK_1_0_definitief.pdf.
44. Zie ook DNB Q&A Toetsingskader Informatiebeveiliging, sheet 30, raadpleegbaar via: https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf.
45. In het Engels: CIA-triad (Confidentiality, Integrity, Availability). Zie ook: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.
46. Zie voor een Amerikaans voorbeeld van een classificatiemethodiek https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Classification-Standard.docx#.
47. Vaak wordt een matrix opgesteld, waarbij de BIV factoren bijvoorbeeld een score Hoog – Midden – Laag krijgen. Een hoge score betekent dat informatie vrijwel permanent beschikbaar moet zijn, dat weinig personen de informatie kunnen bewerken en dat deze informatie vertrouwelijk moet worden behandeld.

entiteiten, en de cyberdreigingen en ICT-kwetsbaarheden beoordelen die relevant zijn voor hun door ICT ondersteunde bedrijfsfuncties en informatie- en ICT-activa. Hier gaat het feitelijk om de identificatie van concrete ICT-risico's. Die zullen verschillen naar gelang de aard van de activiteiten en informatie- en ICT-activa. Een aantal bekende ICT-risico's zijn hacks, installeren van malware, continuïteitsbedreigingen (denk aan een patch op het ene systeem dat verstoringen bij andere gekoppelde systemen veroorzaakt), maar bijvoorbeeld ook onbevoegde toegang en onjuiste autorisaties (bijvoorbeeld mutatierechten terwijl bedoeld is alleen leesrechten te geven). Niet zelfden is menselijk handelen debet aan het materialiseren van een ICT-risico. Verder zullen dus ook eventuele ICT-afhankelijkheden van andere financiële entiteiten beoordeeld moeten worden. Financiële entiteiten moeten regelmatig en ten minste eenmaal per jaar de risicoscenario's die op hen van invloed zijn evalueren.

2.5. Bescherming en voorkoming

Om de ICT-systemen op passende wijze te beschermen en met het oog op de organisatie van responsmaatregelen, dienen financiële entiteiten voortdurend de werking van de ICT-systemen en -instrumenten te monitoren en te controleren, en beperken zij de effecten van deze risico's door de inzet van passende ICT-beveiligingsinstrumenten, -beleidslijnen en -procedures.[48] In artikel 9 lid 2 Verordening wordt in feite een koppeling gelegd met de classificatie uit artikel 8 Verordening: de daar toegekende classificaties moeten feitelijk continu gehandhaafd kunnen worden. Hetzelfde geldt voor de beveiliging van de systemen en data.
Artikel 9 lid 3 en lid 4 Verordening werken verder uit wat er op dit punt van financiële entiteiten wordt verwacht:

- het ontwikkelen en documenteren van een beleid inzake informatiebeveiliging. Naar wij aannemen, kunnen hier maatregelen als het hebben van antivirussoftware en firewalls onder vallen. Een firewall is kort gezegd een soort filter dat bepaalt welke pakketten aan informatie worden doorgelaten of niet;
- het onderhouden van een degelijke structuur voor netwerk- en infrastructuurbeheer om in geval van cyberaanvallen de getroffen informatieactiva te isoleren.[49] Dit is om verdere besmetting van het netwerk en apparatuur te voorkomen. Het is dan wel van belang, de onderlinge afhankelijkheden en koppelingen van systemen te kennen (de 'identificatie' uit artikel 8 Verordening), en dat als het om kritische systemen gaat waar mogelijk een alternatief voorhanden te hebben en backup en restore op orde te hebben (zie verderop in dit artikel over backup en herstel);
- het voeren van een zowel fysiek als logisch (komt neer op: virtueel) toegangsbeleid voor ICT-systemen en -gegevens. Dit betekent in de praktijk, dat enkel bepaalde medewerkers toegang hebben tot bepaalde ruimtes, systemen en data. Fysiek kan dit worden afgedwongen door een toegangspas, virtueel door bepaalde autorisaties (al dan niet) toe te kennen;
- het hanteren van strenge authenticatiemechanismen. Authenticatie is de techniek waarmee een systeem kan vaststellen wie een gebruiker is. Het bekendste voorbeeld van authenticatie is inloggen met een gebruikersnaam en wachtwoord. Andere vormen zijn inloggen met een pas of met een token, multifactor authenticatie (bijvoorbeeld door het sturen van een aanvullende code per sms) of biometrische authenticatie (via een vingerafdruk, gezichtsherkenning of een irisscan)[50];
- het hebben van een change management proces om te garanderen dat alle veranderingen in ICT-systemen op gecontroleerde wijze worden geregistreerd, getest, beoordeeld, goedgekeurd, ingevoerd en geverifieerd;
- beschikken over een passend en alomvattend beleid voor patches en updates. Patching is het doorvoeren van software en firmware aanpassingen.[51] Dit gebeurt niet altijd tijdig en consequent, als gevolg waarvan kwetsbaarheden in de software kunnen blijven bestaan die door aanvallers misbruikt kunnen worden.[52] Hoewel eenduidige cijfers over het percentage aanvallen dat is gebaseerd op verouderde software moeilijk te vinden zijn[53], is wel duidelijk dat het niet tijdig uitvoeren van patches een onnodige vergroting van de beveiligingsrisico's oplevert.

2.6. Detectie

Financiële entiteiten moeten beschikken over mechanismen om afwijkende activiteiten zo spoedig mogelijk te detecteren, met inbegrip van kwesties op

48. Artikel 9 lid 1 Verordening.
49. Dit wordt ook wel "containment" genoemd.
50. Zie onder meer de publicatie van het Nationaal Cyber Security Centrum, onderdeel van het Ministerie van Justitie en Veiligheid, raadpleegbaar via: https://www.ncsc.nl/onderwerpen/authenticatie.
51. Zie voor een voorbeeld van een patch management lifecycle: https://www.manageengine.com/products/desktop-central/help/patch_management/patch_management_life_cycle.html.
52. Eén van de bekendste voorbeelden is de ransomware aanval Wannacry, die gebruik maakte van beveiligingsonvolkomenheden in oudere Windows versies, zie in dit verband: https://www.theguardian.com/technology/2017/jun/14/wannacry-attacks-prompt-microsoft-to-release-updates-for-older-windows-versions.
53. Vaak betreft het hier commerciële consultancy rapporten, zodat er geen goed beeld gevormd kan worden van de gedegenheid van de gebruikte cijfers. Een voorbeeld: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/ noemt een percentage van 75% van aanvallen in 2020 die waren gebaseerd op kwetsbaarheden van ten minste 2 jaar oud.

het gebied van ICT-netwerkprestaties en ICT-gerelateerde incidenten, en om potentiële *single points of failure* te identificeren.[54]
Met detectie verkrijgt een entiteit informatie over het eigen netwerk en de eigen systemen om verdachte gedragingen tijdig te identificeren. Hierbij kan bijvoorbeeld gebruik worden gemaakt van log-informatie van een proxy-, mail- of DNS-server[55], netflow-data, Windows event-logging of log-informatie van antivirus-software op servers en werkstations.[56] Bij onbekende dreigingen kan detectie op basis van afwijkende patronen of gedragingen worden gedaan. Hiervoor kan gebruik gemaakt worden van (zelflerende en al dan niet autonome) algoritmes.[57]
Het doel van deze detectiemechanismen is om meerdere controlelagen mogelijk te maken, alarmmechanismen en criteria om processen voor detectie van en respons op ICT-gerelateerde incidenten in werking te stellen en automatische waarschuwingsmechanismen in te voeren voor de betrokken personeelsleden die belast zijn met de respons op ICT-gerelateerde incidenten.[58]

2.7. Respons en herstel

Artikel 11 Verordening heeft betrekking op respons en herstel. Met respons wordt bedoeld op welke wijze wordt omgegaan met een gedetecteerde bedreiging, met herstel hoe systemen en data weer gebruikt kunnen worden.[59]
In de regel bestaat respons uit meerdere stappen: *containment* (het isoleren van de bedreiging), *eradication* (het verwijderen van de malware), *recovery* (het weer in gebruik nemen van systemen en data), *communication* (zowel intern als extern[60]) en *lessons learned*[61] / eventueel (forensisch) vervolgonderzoek.[62]
Financiële entiteiten zijn verplicht ICT-bedrijfscontinuïteitsplannen in te voeren, te handhaven en deze periodiek te testen.[63] Deze plannen dienen, samen met een ICT-noodherstelplan, ten minste jaarlijks getest te worden.[64] Financiële entiteiten dienen over een functie voor crisisbeheer[65] te beschikken die in geval van activering van het beleid inzake ICT-bedrijfscontinuïteit of van het ICT-noodherstelplan het beheer van interne en externe crisiscommunicatie bepaalt.[66]
De in artikel 11 lid 10 Verordening opgenomen verplichting op verzoek een raming van de geaggregeerde jaarlijkse kosten en verliezen als gevolg van ernstige ICT-gerelateerde incidenten aan de autoriteiten te verstrekken, lijkt ons in de praktijk zeer lastig uitvoerbaar, al is het maar omdat deze kosten en verliezen zelden zeer precies te becijferen zullen vallen.[67]

2.8. Back-upbeleid en herstelmethoden

Financiële entiteiten dienen als onderdeel van hun ICT-risicobeheerkader een back-upbeleid te hebben, waarin nader wordt bepaald op welke gegevens de back-up en de minimale frequentie van de back-up worden toegepast. Daarnaast dienen herstelmethoden (het terugzetten van data en reactiveren van systemen of applicaties) te worden geformuleerd.[68]
Er moeten back-upsystemen worden opgezet die indien vereist kunnen worden geactiveerd in overeenstemming met het back-upbeleid.[69]
Back-ups zijn van belang om dataverlies te compenseren ingeval van storingen of uitval, maar ook in het kader van ransomware aanvallen waarbij gegevens versleuteld worden en pas na betaling van losgeld worden vrijgegeven. Hierbij is wel van belang te onderkennen, dat ook back-ups niet immuun

54. Artikel 10 lid 1 Verordening.
55. Domain Name System: een systeem dat bestaat uit databases die IP-adressen naar domeinnamen omzetten en bijhouden welke websitenamen bij welke IP-adressen horen.
56. Zie onder meer de publicatie van het Nationaal Cyber Security Centrum, onderdeel van het Ministerie van Justitie en Veiligheid, raadpleegbaar via: https://www.ncsc.nl/onderwerpen/detectie/hoe-werkt-detectie
57. https://www.gartner.com/reviews/market/network-detection-and-response geeft een overzicht van enkele aanbieders van dergelijke algoritmes.
58. Artikel 10 lid 2 Verordening.
59. Zie voor een voorbeeld van een Incident Response Plan: https://security.vt.edu/content/dam/security_vt_edu/downloads/incident_response.pdf
60. Denk daarbij aan cliënten, toezichthouders, media, overheid, politie, leveranciers.
61. Zie ook artikel 13 Verordening (Scholing en ontwikkeling) dat feitelijk een dergelijke *lessons learned* cyclus bevat.
62. Zie voor wat verdere toelichting op deze stappen bijvoorbeeld onder meer: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/
63. Artikel 11 lid 4 Verordening.
64. Artikel 11 lid 6 Verordening.
65. Dit moet naar onze mening niet te letterlijk worden genomen, deze functie kan ook worden ondergebracht bij een bestaande functie (Communicatie of Risk Management bijvoorbeeld).
66. Artikel 11 lid 7 Verordening.
67. Een "ernstig ICT-gerelateerd incident" is ingevolge artikel 3 sub 10 Verordening een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen. De "kritieke of belangrijke functie" is op grond van artikel 3 sub 22 Verordening weer een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten. Hier zit natuurlijk een inherent spanningsveld: toezichthouders zullen in de regel sneller van mening zijn dat een ICT incident ernstig is, en zullen ook kennis willen nemen van de twijfelgevallen. Financiële instellingen zullen hier terughoudender zijn. De uitkomsten van het AFM onderzoek naar incidentmeldingen in de asset management sector (https://www.afm.nl/nl-nl/sector/actueel/2021/september/onderzoek-meldplicht-incidenten-asset-managementsector) zullen hier wellicht een verdere inkijk in geven.
68. Artikel 12 lid 1 Verordening.
69. Artikel 12 lid 2 Verordening.

zijn voor dit soort aanvallen. Reeds versleutelde bestanden kunnen ook in de back-up worden geladen, zodat deze ook in de back-up onbruikbaar zijn. Ook kunnen aanvallers eerst de back-up versleutelen[70], alvorens naar de primaire gegevensverwerking te gaan.[71]

2.9. Scholing en ontwikkeling

Artikel 13 Verordening heeft betrekking op scholing en ontwikkeling. Feitelijk gaat het ook over vrijmaken van budget, nu financiële entiteiten capaciteit en personele middelen beschikbaar moeten stellen om informatie te verzamen over kwetsbaarheden en cyberdreigingen, ICT-gerelateerde incidenten en om de gevolgen ervan te analyseren.[72] Verder zit er een element van evalueren in.[73] Dit komt in hoge mate neer op een lessons learned cyclus, waarbij onder meer voorgevallen ICT-incidenten worden onderzocht (post-incidentevaluaties). Hierbij dient naar oorzaken en verbeterpunten gekeken te worden (en die dienen uiteraard te worden doorgevoerd). Dit is snel een omvangrijke en onderhoudsgevoelige cyclus (vooral de status van eerder uitgebrachte aanbevelingen kunnen notoir lange lijsten opleveren), welke cyclus bovendien relatief eenvoudig door de toezichthouder te toetsen valt. De gemaakte veranderingen als gevolg van deze evaluaties moeten op verzoek met de autoriteiten gedeeld worden.[74] Dit is naar onze inschatting een niet te onderschatten verplichting van DORA.
Het leidinggevend ICT-personeel[75] brengt bij het bestuur ten minste jaarlijks verslag uit over de geconstateerde bevindingen en doet aanbevelingen.
Financiële entiteiten ontwikkelen bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele veerkracht als verplichte modules in de opleidingsprogramma's voor het personeel. Deze zijn van toepassing op alle werknemers en het hoger leidinggevend personeel.[76]
Financiële entiteiten houden voortdurend toezicht op relevante technologische ontwikkelingen, ook om inzicht te krijgen in de mogelijke effecten van de invoering van deze nieuwe technologieën op de ICT-beveiligingsvereisten en de digitale operationele veerkracht. Zij blijven op de hoogte van de meest recente processen voor ICT-risicobeheer, om bestaande of nieuwe vormen van cyberaanvallen doeltreffend aan te pakken.[77]

2.10. Communicatie

Als onderdeel van het kader voor ICT-risicobeheer beschikken financiële entiteiten over communicatieplannen die het mogelijk maken ICT-gerelateerde incidenten of ernstige kwetsbaarheden op verantwoordelijke wijze bekend te maken aan cliënten en tegenpartijen en, in voorkomend geval, aan het publiek.[78] Hoofdstuk III van DORA voorziet in nadere eisen ten aanzien van ICT-gerelateerde incidenten, waaronder een meldplicht van 'ernstige ICT-gerelateerde incidenten' aan de toezichthouder.[79]

Communicatie is een niet te onderschatten onderdeel van informatiebeveiliging. Een informatiebeveiligingsincident kan immers eenvoudig leiden tot een verlies van vertrouwen in de betreffende entiteit, al dan niet gevolgd door allerhande gevolg-malheur (media-aandacht, boetes, claims). Informatiebeveiligingsincidenten kunnen op ten minste twee punten afwijken van andere incidenten, namelijk het gegeven dat (a) incidenten vaak als eerste door een ander dan door de entiteit zelf wordt gecommuniceerd (door de aanvaller bijvoorbeeld) en (b) dat incidenten een looptijd van jaren kunnen hebben. Daarmee kan niet per definitie teruggevallen worden op een al klaar liggend crisiscommunicatiehandboek, of althans zal de boodschap concreet moeten zijn.[80]

2.11. Verdere uitwerking van regels

Artikel 15 Verordening vereist van de Europese toezichthouders dat zij een heel aantal van de hiervoor besproken verplichtingen verder uitwerken door middel van *Regulatory Technical Standards*. Daarin zal onder meer een nadere uitwerking worden opgenomen van (i) mechanismen om snelle detectie van afwijkende activiteiten te waarborgen (artikel 10 lid 1 Verordening), (ii) de onderdelen van het ICT-bedrijfscontinuïteitsplan (artikel 11 lid 1 Verordening) en (iii) de onderdelen van de ICT-respons en herstelplannen (artikel 11 lid 3 Verordening).[81] Dit betekent dus dat er aan de toch al gedetailleerde en omvangrijke regels zoals hiervoor op hoofdlijnen besproken,

70. Er bestaan "immutable backups"; backup bestanden die niet gewijzigd kunnen worden. Het is ons niet bekend hoe immutable deze backups daadwerkelijk zijn.
71. Zie onder meer de publicatie van het Nationaal Cyber Security Centrum, onderdeel van het Ministerie van Justitie en Veiligheid, raadpleegbaar via: https://www.ncsc.nl/actueel/weblog/weblog/2021/back-up.
72. Artikel 13 lid 1 Verordening.
73. Artikel 13 lid 2 Verordening.
74. Artikel 13 lid 3 Verordening.
75. Artikel 13 lid 5 Verordening. Uiteraard moet bekend zijn bij wie dergelijke verplichtingen ondergebracht worden, zeker als er binnen de organisatie niet voorzien is in een specifieke IT verantwoordelijke binnen het hoger leidinggevend personeel
76. Artikel 13 lid 6 Verordening.
77. Artikel 13 lid 7 Verordening. Ook van deze verplichtingen is het de vraag hoe kleinere organisaties, niet zijnde micro-ondernemingen, met weinig of geen specifieke (ICT) informatiebeveiligingsfunctionarissen, hieraan dienen te voldoen.
78. Artikel 14 lid 1 Verordening.
79. Artikel 19 lid 1 Verordening.
80. Zie voor verdere achtergrond de publicatie van MIT Technology Review, raadpleegbaar via: https://www.technologyreview.com/2016/04/20/160885/crisis-communication-after-an-attack/.
81. Zie in dit verband tevens de door de Europese toezichthouders gegeven uitleg zoals genoemd in voetnoot 7.

nog meer detail wordt toegevoegd. Zoals in paragraaf 1.2 aangegeven gaan we de komende maanden de eerste voorstellen zien vanuit de Europese toezichthouders.

3. DNB en AFM

Op dit moment zijn de regels voor financiële entiteiten op het gebied van ICT-risicobeheer in Nederland versnipperd en verschillen per type instelling, afhankelijk van DNB- of AFM-toezicht. Deze bestaande regels bepalen ten dele ook hoe groot de stap zal naar DORA-compliance. We staan daar hieronder kort bij stil.

Op basis van artikel 3:17 Wet op het financieel toezicht ("Wft") dienen instellingen onder toezicht van DNB te beschikken over adequate procedures en maatregelen ter beheersing van IT-risico's. Het gaat hierbij onder meer om het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van geautomatiseerde gegevens. Adequaat betekent in dit verband dat de procedures en maatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur.[82]

Ter invulling van deze bepaling heeft DNB Good Practices op het gebied van informatiebeveiliging gepubliceerd.[83] Dit is een vrij uitvoerige (84 pagina's) en vaak gedetailleerde beschrijving van informatiebeveiligingsrisico's en beheersmaatregelen, die veel raakvlakken met ISO 27001 kent. Er is sprake van een behoorlijk mate van overlap met DORA.

Ook de AFM heeft over informatiebeveiliging gepubliceerd, onder meer via de Principes voor informatiebeveiliging.[84] Dat is een aanzienlijk korter (15 pagina's) en veel minder gedetailleerd uitgewerkt document dan dat van DNB.

Financiële entiteiten die onder toezicht van DNB staan en die de DNB Good Practices deugdelijk hebben geïmplementeerd, zullen op veel punten al een goede voorbereiding op DORA hebben of daar op onderdelen zelfs al op het vereiste niveau zitten. Voor partijen die de DNB Good Practices slechts gedeeltelijk hebben geïmplementeerd dan wel die zich tot de AFM Principes hebben beperkt, zal naar onze inschatting nog de nodige uitbreiding, verdieping en concretisering nodig zijn.

4. Verenigde Staten

Ook in de Verenigde Staten zijn er initiatieven met betrekking tot wet- en regelgeving op het gebied van informatiebeveiliging. De Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") uit maart 2022[85] verplicht ondernemingen uit sectoren die als kritische infrastructuur zijn aangemerkt – de financiële sector is als kritisch aangemerkt – om informatiebeveiligingsincidenten te melden bij het Cybersecurity and Infrastructure Security Agency ("CISA").[86] Informatiebeveiligingsincidenten moeten binnen 72 uur gemeld worden; als het echter om ransomware gaat is de meldingstermijn 24 uur.[87] CISA kan dan weer hulp bieden bij aanvallen, aanvalspogingen analyseren en andere relevante ondernemingen waarschuwen.

De US Securities and Exchange Commission ("SEC") kwam eveneens in maart 2022 naar buiten met een voorstel voor een Rule op het gebied van informatiebeveiliging.[88] In het kort verplicht deze Rule[89] beursgenoteerde ondernemingen om materiële cybersecurity incidenten te melden aan de SEC, maar ook om periodiek bepaalde informatie openbaar te maken. [90] Dit betreft:

- De procedures die de onderneming heeft om informatiebeveiligingsrisico's te identificeren en te beheersen;
- De rol van het management bij het implementeren van dergelijke procedures;
- De expertise ten aanzien van informatiebeveiliging binnen het bestuur[91] en de wijze waarop het bestuur overzicht houdt op dit risico;
- De opvolging van eerder gerapporteerde informatiebeveiligingsincidenten.

Het doel van deze Rule is om beleggers in de betreffende ondernemingen te informeren over het risicomanagement, strategie en governance van de onderneming, en om ervoor te zorgen dat beleggers tijdig informatie over informatiebeveiligingsincidenten ontvangen.

Opvallend is dat de CIRCIA en genoemde SEC Rule vooral betrekking hebben op het rapporteren en delen van informatie, en veel minder op governance en risicomanagement zoals DORA. Mogelijk is de achterliggende gedachte dat deze rapportage- en informatieverplichtingen as het ware vanzelf dwingen tot solide governance en risicomanagement.

82. Zie voor een verdere toelichting de website van DNB, raadpleegbaar via: https://www.dnb.nl/voor-de-sector/open-boek-toezicht-fasen/lopend-toezicht/prudentieel-toezicht/governance/q-a-informatiebeveiliging/
83. Raadpleegbaar via: https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf
84. Raadpleegbaar via: https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging
85. De wet is nog niet van kracht: afgaande op de CISA website (https://www.cisa.gov/circia) kan dat nog 42 maanden duren vanaf maart 2022.
86. Zie de website van CISA voor verdere toelichting, raadpleegbaar via: https://www.cisa.gov/circia.
87. Een al dan niet bedoeld neveneffect zal zijn, dat het onder de radar betalen van losgeld erg lastig wordt.
88. Zie het betreffende nieuwsbericht, raadpleegbaar via: https://www.sec.gov/news/press-release/2022-39
89. Zie voor een verdere toelichting de publicatie van de SEC: https://www.sec.gov/rules/proposed/2022/33-11038.pdf
90. https://www.sec.gov/files/33-11038-fact-sheet.pdf
91. De SEC merkt hier fijntjes op: "if any".

Het is interessant om te zien hoe de ontwikkelingen in de Verenigde Staten zullen zijn, nu daar een andere insteek lijkt te worden gekozen ten aanzien van informatiebeveiliging dan de Europese Unie dat doet, en of die verschillen duurzaam zijn. Bij de Algemene Verordening Gegevensbescherming lijkt er sprake van enige "import" van die regels door de Verenigde Staten; mogelijk gebeurt dat met DORA ook.

5. Conclusies

DORA is een omvangrijk en gedetailleerd wetgevingspakket. In dit artikel hebben we slechts één pijler op hoofdlijnen besproken, waarbij die eisen ook nog eens nader uitgewerkt zullen gaan worden in lagere regelgeving. Financiële entiteiten moeten hun borst dus nat maken voor DORA. Bestuurders van financiële entiteiten moeten de impact ervan zeker niet onderschatten. En dat in een tijd dat er toch al genoeg uitdagingen zijn op het gebied van regelgeving, zoals de duurzaamheidsregelgeving en anti-witwasregelgeving. Wij constateren in ieder geval een aantal concrete aandachtspunten voor financiële entiteiten in de voorbereiding op DORA.

Hoewel DORA voor een aantal specifieke marktspelers voorziet in een verlicht regime, blijft DORA voor het overgrote deel van de markt een *one-size-fits-all* raamwerk. We zien in de implementatie van DORA met name grote uitdagingen voor de wat kleinere financiële entiteiten. Onze zorg gaat dan vooral uit naar de asset managementsector. Dat zijn veelal kleinere ondernemingen die al grote moeite hebben om alle ontwikkelingen op het gebied van wet- en regelgeving bij te benen.[92] Bovendien gelden voor hen nog 'slechts' de AFM Principes voor informatiebeveiliging die veel minder ver gaan dan de DNB Good practice. Anders gezegd, voor de AFM-instellingen is de sprong naar DORA een veel grotere. Zij zullen mogelijk op onderdelen een beroep op proportionaliteit kunnen doen en zullen dit alsdan grondig moeten onderbouwen. Juist ook voor hen loont het om tijdig met voorbereiding te beginnen: alleen bij een goed begrip van de totale potentiële impact, kan zorgvuldig een beroep op proportionaliteit gedaan worden. Tegelijkertijd zal voor veel grotere financiële entiteiten juist gelden dat zij een veel hogere ICT-verwevenheid hebben binnen hun processen. Daar ligt nadrukkelijk een uitdaging in de identificatie van al die processen en vaststelling van beheersmaatregelen zonder het overzicht te verliezen dan wel te verzanden in bureaucratie.

DORA vereist nadrukkelijk dat compliance met de Verordening tot de taken van het bestuur van de financiële entiteit moet behoren. Dit is een trend die we ook bij andere wetgeving ontwaren, zoals anti-witwasregelgeving.[93] De vraag is uiteraard of de raden van bestuur van Nederlandse financiële entiteiten daar wel voldoende voor geëquipeerd zijn, in termen van kennis en ervaring en omvang. Om toch goed beslagen ten ijs te komen vereist dit naar ons oordeel dat bestuurders ook nu al actief kennis nemen van DORA en zelf betrokken zijn bij de implementatie. Alleen dan kunnen zij straks met goed recht zeggen voldoende kennis van en ervaring met het onderwerp te hebben, adequaat te kunnen budgetteren en controle te hebben over compliance met DORA.

ICT-risicobeheer *an sich* is een aparte discipline. Dat doet de compliance of risk officer er niet 'zomaar even bij'. Wat dat betreft zien wij een parallel met de duurzaamheidsregelgeving die langzaam maar zeker over de financiële sector wordt uitgerold: ook dat is een aparte discipline, vereist specifieke kennis die niet vanzelfsprekend aanwezig is, en vraagt aldus om investeringen in personele en technische middelen. Dat geldt naar onze mening voor DORA net zo goed. Het devies voor financiële entiteiten: weet wat je niet weet, en investeer tijdig in de vereiste middelen om die gap te beslechten.

Teneinde compliance met DORA aantoonbaar en toetsbaar te waarborgen, zullen financiële entiteiten moeten overgaan tot de vaststelling van een uitgebreid raamwerk van beleid en procedures. DORA vereist op veel onderdelen een vorm van beleid, vastlegging en aantoonbare evaluatie, waarvan de uitkomsten ook nog eens met de toezichthouder gedeeld moeten kunnen worden. Er komt aldus weer een hoop papierwerk bij voor financiële entiteiten. We raden marktpartijen aan tijdig te identificeren wat er precies vereist zal zijn om de voorbereiding behapbaar te maken.

92. Zie bijvoorbeeld AFM Trendzicht 2023, p. 45 (https://www.afm.nl/nl-nl/over-de-afm/verslaglegging/trendzicht), waarin de consolidatietendens in de Nederlandse vermogensbeheermarkt wordt benoemd.

93. Zie bijvoorbeeld de Richtsnoeren van EBA met betrekking tot de AML compliance officer (EBA/GL/2022/05, 14 juni 2022), meer specifiek de richtsnoeren ten aanzien van het leidinggevend orgaan (richtsnoer 4.1).